Office of Information Technology Services

Service Level Agreement

Intrusion Prevention Service (IPS)

November 12, 2013 v2.1

Intrusion Prevention Service (IPS)

Service Description

Intrusion Prevention Service (IPS) provides a critical defensive layer of security for the customer's network that monitors network activities for malicious behavior and can block or prevent those activities. This service option is a fully managed Internet Protocol (IP) based security solution that protects against threats from hackers, viruses, and worms that attack customer networks and computing equipment. ITS manages all phases of the service, including consultation for the required policies, implementation, operations, and ongoing configuration management.

Service Commitments

The general areas of support (such as Incident and Change Management) applicable to every ITS service, are specified in the ITS Global Service Levels document.

IPS Service Availability Targets:

- Target Service Availability is 99.9%.

Hours of Availability

- This service is available to customers 24 x 7 and adheres to the maintenance window schedule listed in the ITS Global Service Levels document.

ITS Responsibilities

- Service provisioning occurs within 45-60 days from the date of the consultation meeting signoff
- ITS will conduct a design and consultation session with the customer
- ITS will configure and support the IPS device installed at the customer premise, and will perform continual tuning of security policies
- ITS will store customer IPS event logs and retain the logs for a period of 1 month
- ITS will maintain the installed IPS device with the latest security patches and software releases, according to vendor recommendations
- Signature updates are performed once the updates have been tested and approved, and are implemented via the change control process. Customers may opt for “zero-day” updates for their IPS device, whereby updates are applied as soon as they are released by the vendor.
- ITS will implement customer notification of pre-identified critical events

- 24 x 7 centralized monitoring and management via ITS Network-Security Operations and the ITS Service Desk

Customer Responsibilities

- Consents to pay the OSBM-approved rate for the term of this agreement. This agreement will be in effect for three years from the date service is declared operational. This agreement will be automatically renewed on a month-to-month basis thereafter.
- Perform a security vulnerability assessment and a risk analysis of the agency environment, prior to the initial consultation
- Provide a secure physical facility with access control restrictions for the placement of the Intrusion Prevention Service components, preferably co-located with the ITS provided WAN Service router
- The secure facility requires customer coordinated 24 x 7 accessibility for authorized ITS staff
- Provide a 24 x 7 point of contact (POC) for ITS to contact for reporting and coordinating outages or emergency maintenance
- The POC list will include the only authorized contacts for security related issues, including the approval of the initial security policy and requesting policy changes
- The Agency IPS Service option requires an Agency Security Point of Contact
- Contact the ITS Service Desk to report problems or request assistance
- Work with ITS on a mutually agreed schedule to allow required maintenance services to be performed in a timely manner
- Provide ITS all required access to IPS device, if placement is behind a non-ITS managed firewall

Service Level Agreement Scope

This agreement specifies only the standard operational service commitments and responsibilities of ITS and its customers. Customer-specific deviations from these commitments and responsibilities will be specified in an accompanying Memorandum of Understanding. Service rates are outside the scope of this agreement and are specified in financial documents.

Signatures of Approval and Agreement Date

Customer Signatures

Agency Head or Designee:

Name	Title	Signature	Date

Agency Chief Financial Officer:

Name	Title	Signature	Date

ITS Signature

State Chief Information Officer:

Name	Title	Signature	Date
Chris Estes	State CIO		